SECURE DISK DRIVE COMPRISING A SECURE DRIVE KEY AND A DRIVE ID FOR IMPLEMENTING SECURE COMMUNICATION OVER A PUBLIC NETWORK

ABSTRACT OF THE DISCLOSURE

A secure disk drive is disclosed comprising a disk for storing data, and an input for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a client drive ID identifying the client disk drive. The secure disk drive comprises a secure drive key and an internal drive ID. A key generator within the secure disk drive generates a client drive key based on the client drive ID and the secure drive key, and an internal drive key based on the internal drive ID and the secure drive key. The secure disk drive further comprises an authenticator for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator is responsive to the encrypted message and the client drive key. The secure disk drive further comprises a data processor comprising a message input for receiving the encrypted message from the client disk drive, and a data output for outputting the ciphertext data to be written to the disk. The data processor further comprises an enable input for receiving the enable signal for enabling the data processor, and a key input for receiving the internal drive key, the internal drive key for use in generating a message authentication code. The data processor outputs reply data comprising the message authentication code. The secure disk drive outputs a reply to the client disk drive, the reply comprising the reply data and the internal drive ID.